

CYRIS360

Cybersecurity Engineering

November 2025 – Version 1.4

Unleashing Cyber Resilience in Every Direction.

Cybersecurity Engineering

Overview

01	Secure IoT & Cyber Resilience Act (CRA)
02	Security Testing
03	Secure Automotive
04	Secure EV Charging
05	Secure AI Lifecycle
06	Business cases
06.1	CSMS implementation - Automotive

1. Secure IoT & Cyber Resilience Act (CRA)

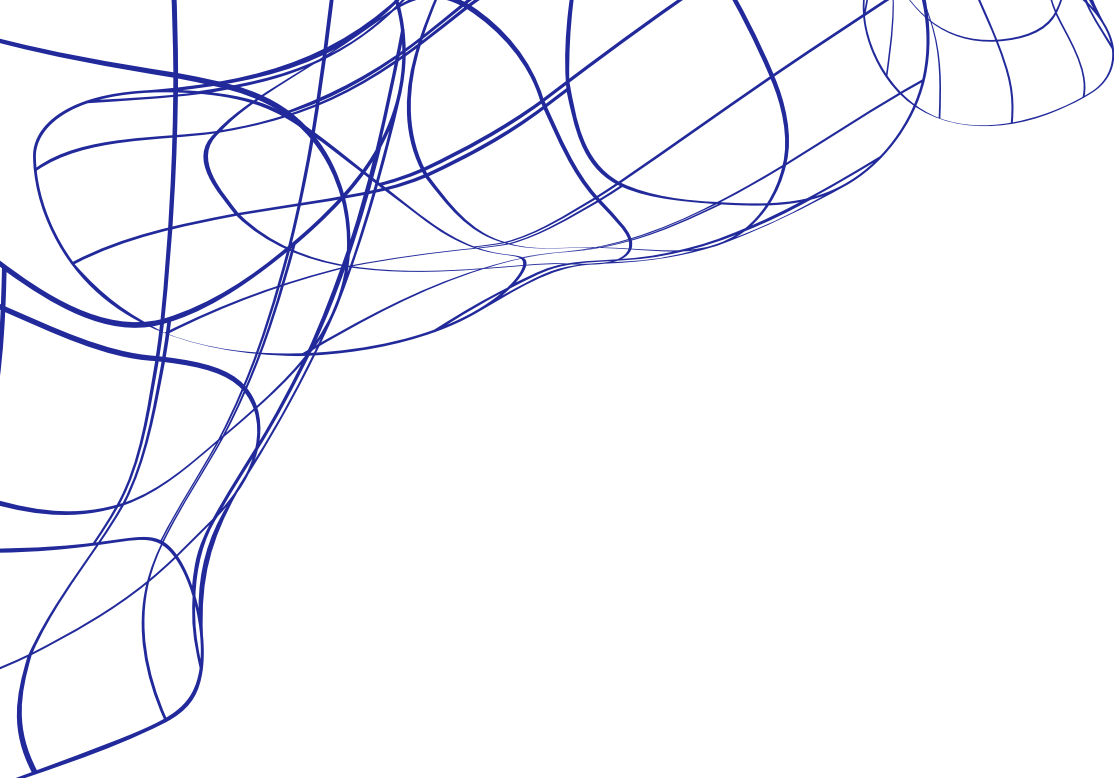
Standards

- ISO/IEC standards:
ISO/IEC274xx Series
ISA/IEC 62443 Framework
- ETSI standards:
EN 303 645
- SESIP: EN17927

Conformity assessment

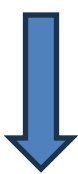
- Evaluation methods:
Default: (Basic) Self-assessment
Important: 3rd party assessment
Critical: EUCC certification
- Target of Evaluations
Doorbell, home appliance, IP Camera,
Printer, Inverter, etc.





Secure Software Development Lifecycle

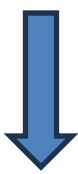
Step 1



Design

Security requirements
Threat Modelling

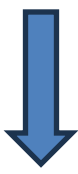
Step 2



Implement

Code Review (SAST, DAST, Secret scan)
Software Composition Analysis (SCA)

Step 3



Build & Release

Application Signature
Secret Management

Step 4

Operate

Vulnerability Management
Secure Software Update



2. Security testing

Black box testing

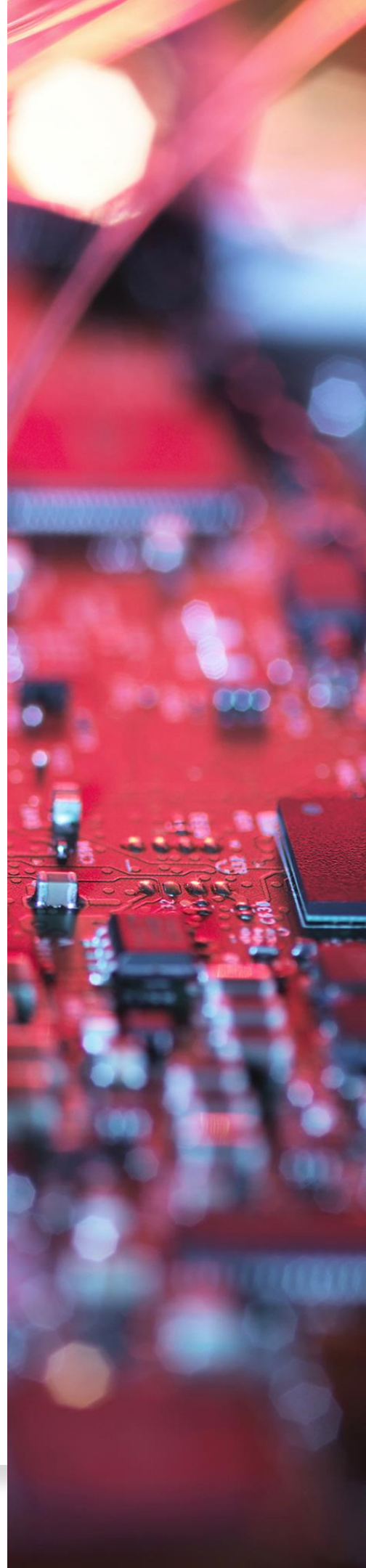
Time-boxed security scan of trust boundaries and communication interfaces.

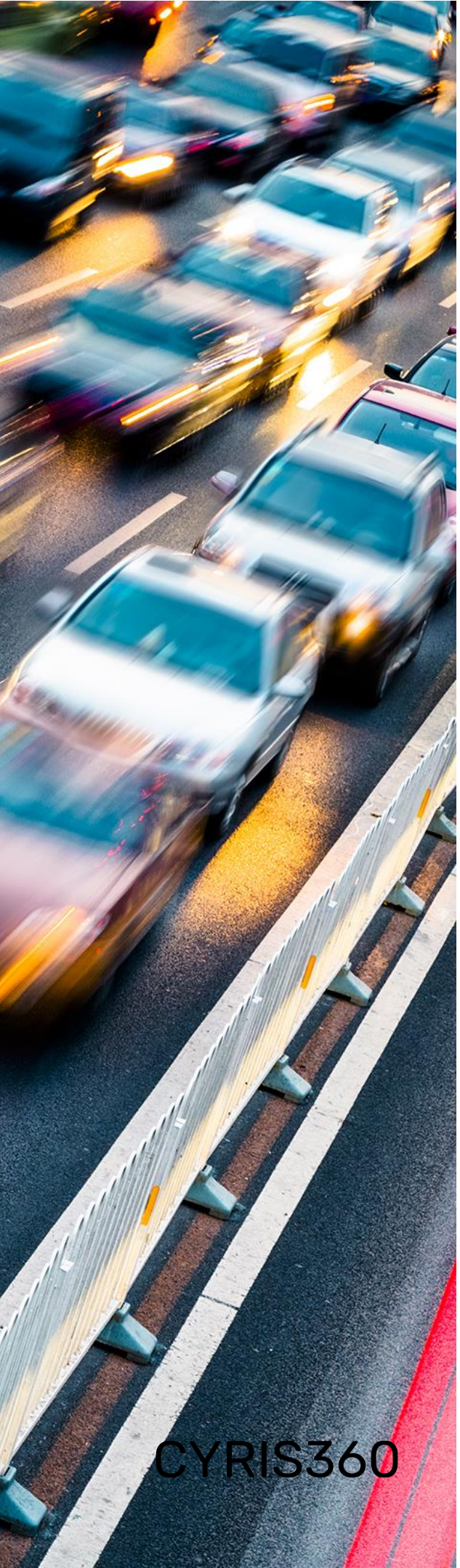
Requirement-based testing

Security testing according to predefined test plan.

Reverse engineering & Side channel analysis

Secret extraction from mobile applications & hardware secure element / trusted module.





3. Secure Automotive

UN R155 & ISO/SAE 21434 (CSMS)

- Implementation of CSMS requirements
- Maintain the CS Interface Agreement
- Maintain the TARA

Secure onboard communication (SecOC)

- Secure Wireless Interfaces (Wi-Fi, BLE, etc.)
- Secure Ethernet (MACsec, IPSec, TLS)
- Secure EV Charging (ISO15118)

In partnership with



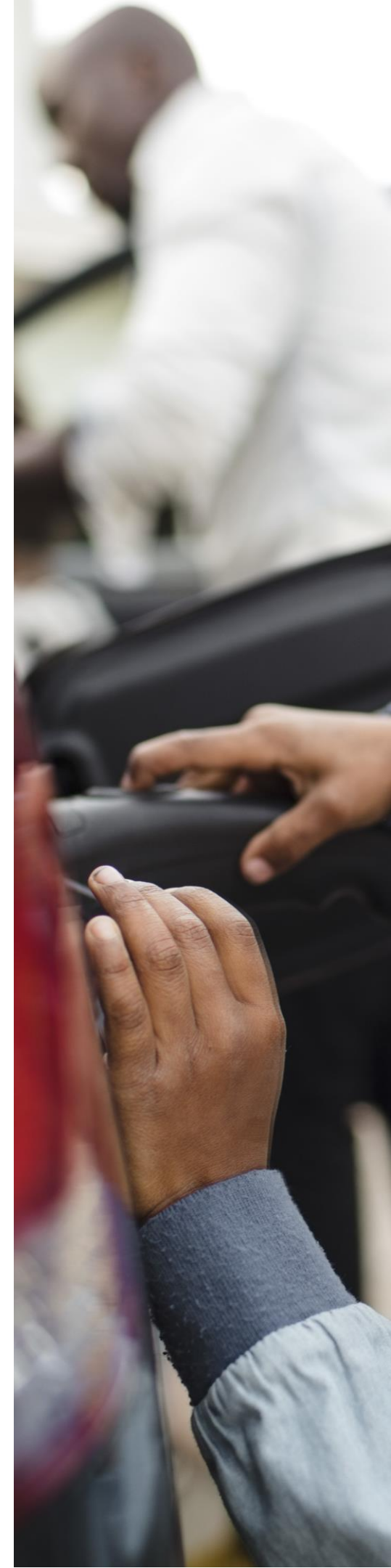
4. EV Charging & V2G

Standards

- ISO/IEC standards:
ISO/IEC274xx Series
ISA/IEC 62443 Framework
- ETSI standards:
EN 303 645
- SESIP: EN17927

Conformity assessment

- Evaluation methods:
Default: (Basic) Self-assessment
Important: 3rd party assessment
Critical: EUCC certification
- Target of Evaluations
Doorbell, home appliance, IP Camera,
Printer, Inverter, etc.



5. Secure AI Lifecycle

AI Risk Assessment

Threat modeling:

- System security & Access control
- Data governance & Integrity
- Protection of Intellectual property
- Third-party components
- Readiness for business continuity

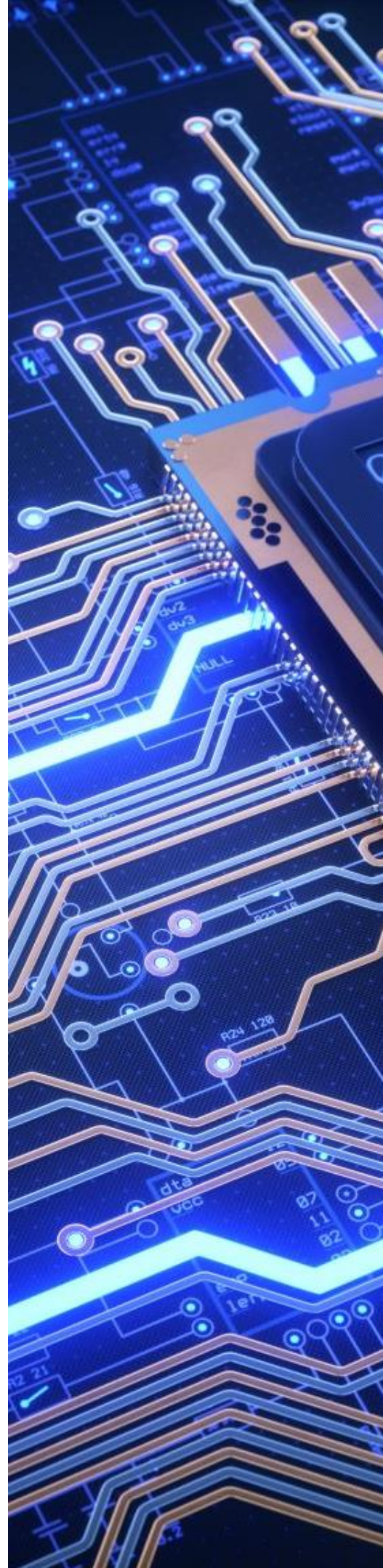
Reference frameworks & standards:

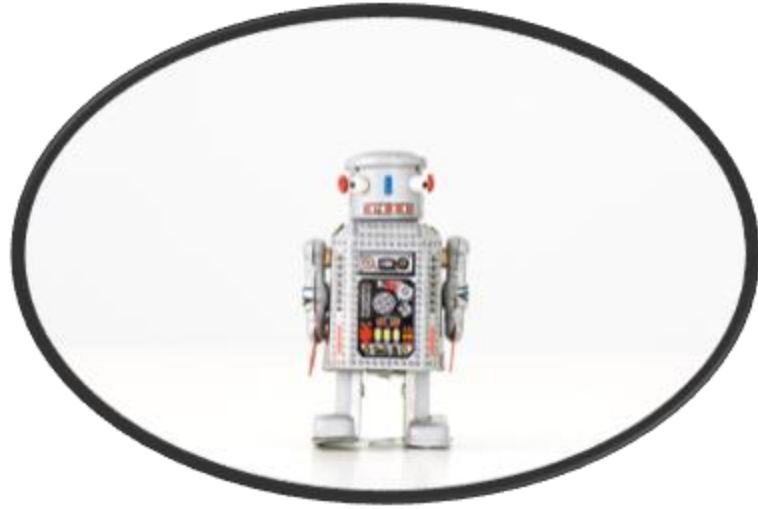
- OWASP ML & LLM Top 10
- Google Secure AI Framework
- ISO/IEC5338
- ETSI SAI – EN 304 223

AI Security Testing

Attack scenarios:

- Prompt injection
- Evasion
- Model/Data poisoning
- Model theft & Training Data leak





6. Business Cases



CYRIS360



CSMS implementation – Tier-1 Supplier

Initial Situation

Automotive Tier-1 supplier

- Software running on critical automotive component for EV.
- The OEM has a cybersecurity interface agreement with the supplier.
- The supplier is entirely dependent on the automotive market.

Challenge

UNR 155 & CSMS requirements

- The deadline to implement the ISO/SAE21434 requirement is approaching.
- The OEM can only rely on suppliers that did not implement the relevant CSMS requirements.
- Lack of in-house expertise to implement the relevant requirements.

Result

CSMS implementation

- Leverage overlap with other management systems (Information Security, Safety, Quality)
- Established the CSMS documentation
- Defined the roles and responsibilities.
- Performed a TARA
- Review and approval by independent party (UTAC)



Do you have any questions?

Let us know: we are happy to help!

CYRIS360

✉ info@cyris360.com

🌐 www.cyris360.com

